

| NODIS Library | Legal Policies(2000s) | Search |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

[Request Notification of Change](#) (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

Preface

P.1 Purpose

This National Aeronautics and Space Administration (NASA) Procedures and Requirements (NPR) document implements the NASA Policy Directive (NPD) 2810.1, NASA Information Security Program. NPR 2810.1 establishes the procedures and requirements of the NASA Information Technology (IT) Security Program and provides direction designed to ensure that safeguards for the protection of the confidentiality, integrity, and availability of unclassified IT resources are integrated into and support NASA's missions, functional lines of business, and infrastructure based on risk-managed, cost-effective IT security and information security principles and practices.

P.2 Applicability

P.2.1 This NPR applies to all NASA employees, NASA support service contractors, NASA IT resources, and in NASA contracts, grants, purchase orders, and cooperative agreements, where appropriate, in achieving Agency missions, programs, projects, and institutional requirements. Facilities, resources, and personnel under a contract or part of a grant, an international partner agreement, or a volunteer associate's agreement from NASA to a college, university, research establishment, or associate's program are included in the applicability of this document unless specific sections are identified as

being waived in the contract, grant, or cooperative agreement.

P.2.2 These procedures and requirements shall be implemented for unclassified NASA information and IT resources that are contracted out or outsourced to (1) another Center; (2) another Government Agency; (3) a Government owned, contractor operated (GOCO) facility; (4) partners under the Space Act; (5) partners under the Commercial Space Act of 1997; or (6) commercial or university facilities. These entities shall be subject to IT security compliance reviews and audits by NASA. Waivers to specific procedures and requirements shall be approved by the cognizant Mission Directorate, Center, or Headquarters Chief Information Officer (CIO) and by the NASA Office of the Chief Information Officer (OCIO).

P.2.3 Any IT resource in or behind the NASA assigned Internet Protocol (IP) address space shall follow NASA and Center policies and requirements and shall be subject to IT security compliance reviews and audits by NASA or its agents. Contractor, grant, international partner's, or research facility's computing and information resources that do not possess NASA information or IT resources, and that are not under direct NASA management cognizance, or are merely incidental to a contract, (e.g., a contractor's payroll and personnel system) are normally excluded from full review or audit to protect proprietary or privacy data.

P.2.4 These procedures and requirements do not apply to Classified National Security Information (CNSI). Specific policy and requirements for CNSI is contained in NPD 1600.2, NASA Security Policy, and NPR 1600.1, NASA Security Program Procedural Requirements.

P.2.5 For purposes of this NPR, NASA Headquarters is treated as a Center. Thus, all roles and responsibilities of the Center CIO are also applicable to the NASA Headquarters CIO. Further, all stipulated Center requirements are also applicable to NASA Headquarters.

P.3 Authority

- a. 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended.
- b. 5 U.S.C. 552, et seq., the Freedom of Information Act, as implemented by 14 Code of Federal Regulations (CFR) 1206.
- c. 5 U.S.C. 552a, the Privacy Act, Pub. L 93-579, as amended.
- d. 18 U.S.C. 799, Violation of Regulations of National Aeronautics and Space Administration.
- e. 18 U.S.C. 2510, et seq., the Electronic Communications Privacy Act of 1986, as amended.
- f. 22 U.S.C. 2751, et seq., the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations, 22 CFR Parts 120-130.
- g. 40 U.S.C. § 11101 et seq., Clinger-Cohen Act of 1996.
- h. 42 U.S.C. 201 nt., Health Insurance Portability and Accountability Act of 1996, as amended.

- i. 44 U.S.C. 101, E-Government Act of 2002.
- j. 44 U.S.C. 3535, Federal Information Security Management Act (FISMA) of 2002.
- k. 44 U.S.C. 3501, et seq., Paperwork Reduction Act of 1995, as amended.
- l. 50 U.S.C. Appendix 2401-2420, Export Administration Act of 1979, as amended.
- m. 14 CFR Part 1206, Availability of Agency Records to Members of the Public.
- n. 15 CFR Parts 730-774, Export Administration Regulations.
- o. 22 CFR Parts 120-130, International Traffic in Arms Regulations.
- p. EO 12958, Classified National Security Information, dated April 17, 1992.
- q. EO 13011, Federal Information Technology, dated July 16, 1996.

P.4 References

- a. OMB Circular No. A-130, Appendix III Management of Federal Information Resources dated November 28, 2000.
- b. OMB Circular A-11, Planning, Budgeting and Acquisition of Capital Assets, dated July 16, 2004.
- c. OMB Memorandum M-00-13, Privacy Policies, and Data Collection on Federal Web Sites, dated June 22, 2000.
- d. National Telecommunications and Information System Security (NTISS) 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems, dated June 17, 1982.
- e. NTISS 100, National Policy on Application of Communications Security to Command Destruct Systems, dated February 17, 1988.
- f. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection, dated December 17, 2003.
- g. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM).
- h. NPD 1382.17, NASA Privacy Policy.
- i. NPD 1440.6, NASA Records Management.
- j. NPR 1441.1, NASA Records and Retention Schedules.
- k. NPR 1600.1, NASA Security Program Procedural Requirements.
- l. NPD 1600.2, NASA Security Policy.
- m. NPR 1620.2, Physical Security Vulnerability Risk Assessments.
- n. NPD 2540.1, Personal Use of Government Equipment Including IT
- o. NPR 2800.1, Managing Information Technology.
- p. NPD 2810.1, NASA Information Security Policy.

- q. NPD 2820.1, NASA Software Policy.
- r. NPR 2830, NASA Enterprise Architecture.
- s. NPR 7100.1, Protection of Human Research Subjects.
- t. NPR 7100.8, Protection of Human Research Subjects.
- u. NPR 7100.10, Curation of Extraterrestrial Materials.
- v. NPR 7120.4, Program/Project Management.
- w. NPR 7120.5, NASA Program and Project Management Processes and Requirements.
- x. NPR 7120.6, Lessons Learned Process.
- y. NPR 7150.2, NASA Software Engineering Requirements.
- z. NPR 8000.4, Risk Management Procedural Requirements.
- aa. NPR 9900.1, Counterintelligence Procedures and Guidelines.
- bb. Federal Information Processing Standards (FIPS). URL:
<http://csrc.nist.gov/publications/fips/index.html>.
- cc. National Institute of Standards and Technology (NIST) Special Publications (SPs) 800 Series. URL: <http://csrc.nist.gov/publications/nistpubs/index.html>.

P.5 Cancellation

- a. NPR 2810.1, Security of Information Technology, revalidated August 12, 2004.
- b. NITR 2810-1, Wireless Requirements, dated September 15, 2003.
- c. NITR 2810-2, Information Technology (IT) System Security Requirements, dated June 28, 2004.
- d. NITR 2810-3, NASA Internet Publishing Guidelines, dated December 2, 2004.
- e. NITR 2810-4, Information Technology (IT) System Security Certification and Accreditation and Authorizing Systems for Operation, dated December 21, 2004.
- f. NITR 2810-5, Information Technology (IT) Security Patch Management System, dated December 14, 2004.

/S/

Patricia Dunnington
Chief Information Officer

DISTRIBUTION: NODIS

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |

[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) || [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |**DISTRIBUTION:**
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
